Docket No. AUS920030349US1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Kirkland**	§	
	§	Confirmation No.: **6018**
Serial No. **10/607,515**	§	
	§	Group Art Unit: **2131**
Filed: **June 26, 2003**	§	
	§	Examiner: **LaForgia, Christian A.**
For: **Wireless Bridge Device for Secure, Dedicated Connection to a Network**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on September 24, 2007.

A fee of $510.00 is required for filing an Appeal Brief. Please charge this fee to Yee & Associates, P.C. Deposit Account No. 50-3157. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees, which may be required to Yee & Associates, P.C. Deposit Account No. 50-3157.

A one-month extension of time is believed to be necessary. I authorize the Commissioner to charge the one-month extension fee of $120.00 to Yee & Associates, P.C. Deposit Account No. 50-3157. No additional extension of time is believed to be necessary. If, however, an additional extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to Yee & Associates, P.C. Deposit Account No. 50-3157.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation of Armonk, New York.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-20

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 10, 11, and 17.
2. Claims withdrawn from consideration but not canceled: None.
3. Claims pending: 1-9, 12-16, and 18-20.
4. Claims allowed: None.
5. Claims rejected: 1-9, 12-16, and 18-20.
6. Claims objected to: None.

C. CLAIMS ON APPEAL

The claims on appeal are: 1-9, 12-16, and 18-20.

STATUS OF AMENDMENTS

An Amendment after Final Office Action was not filed. Therefore, the claims on appeal herein are as presented in the Response to Office Action dated May 9, 2007.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

The subject matter of claim 1 is directed to a data processing configuration that includes a data processing system. A network communication device (**202**, **Figure 2**, page 4, lines 20-22) of the data processing system (**221**, **Figure 2**, page 4, lines 19-22) enables the data processing system to communicate with a wired network (**107**, **Figure 2**, page 5, lines 17-19). The network communication device includes a wired port (**231**, **Figure 2**, page 5, lines 4-7) for receiving a cable connector. The data processing configuration also has a first wireless bridge device (**232A**, **Figure 2**, page 5, lines 13-17, **Figures 3A** and **3B**, page 6, lines 4-6) having a cable connector for insertion in the wired port of the network communication device, wherein the first wireless bridge device further includes an encryption unit (**350**, **Figure 3B**, page 6, lines 12-14) for encrypting information received from the data processing system according to a predetermined encryption algorithm and a transmitter for transmitting the encrypted information wirelessly (**344**, **Figure 3A**, page 6, line 7), and a second wireless bridge device (**232B**, **Figure 2**, page 5, lines 13-17, **Figures 3A** and **3B**, page 6, lines 4-6) having a cable connector for insertion into a port (**234**, **Figure 2**, page 5, lines 13-17) of the wired network, wherein the second wireless bridge device includes a receiver (**346**, **Figure 3A**, page 6, line 7) for receiving encrypted information transmitted wirelessly from the first wireless bridge device, and a decryption unit (**360**, **Figure 3B**, page 6, lines 20-22) for decrypting the received encrypted information according to a decryption algorithm that is matched to the encryption algorithm of the first wireless bridge device, wherein the first and second wireless bridge devices communicate exclusively with each other in a wireless manner.

B. CLAIM 8 – INDEPENDENT

The subject matter of claim 8 is directed to a wireless bridge suitable for use in a data processing network. The wireless bridge includes a first wireless bridge device (**232A**, **Figure 2**, page 5, lines 13-17, **Figures 3A** and **3B**, page 6, lines 4-6) configured to receive network packets from a network communication device, encrypt the network packets according to an encryption algorithm, and transmit the encrypted packets wirelessly, wherein the first wireless bridge device

includes an RJ-45 connector (**231**, **Figure 2**, page 5, lines 4-7) suitable for connecting to an Ethernet compliant NIC. The wireless bridge also includes a second wireless bridge device (**232B**, **Figure 2**, page 5, lines 13-17, **Figures 3A** and **3B**, page 6, lines 4-6) configured to receive encrypted network packets from the first wireless bridge device and decrypt the packets according to a decryption algorithm, wherein the second wireless bridge device is configured to be connected to an RJ-45 port (**234, Figure 2**, page 5, lines 13-17) of a wired local area network (**107**, **Figure 2**, page 5, lines 17-19), wherein the encryption and decryption algorithms of the first and second wireless bridge devices are unique and matched to each other wherein the first wireless bridge device is capable of communicating information exclusively to the second wireless bridge device and the second wireless bridge device is capable of decoding information exclusively from the first wireless bridge device.

C. CLAIM 15 – INDEPENDENT

The subject matter of claim 15 is directed to a method of enabling wireless connection between a data processing device and a local area network. The method includes providing a first wireless bridge device configured to receive network packets from a network device, encrypt the packets according to an encryption algorithm, and transmit the encrypted packets wirelessly (**232A**, **Figure 2**, page 5, lines 13-17, **Figures 3A** and **3B**, page 6, lines 4-6, page 3, lines 1-17). The method also includes providing a second wireless bridge device configured to receive encrypted network packets from the wireless bridge device and decrypt the packets according to a decryption algorithm wherein the encryption and decryption algorithms of the first and second wireless bridge devices are unique and matched to each other wherein the first wireless bridge device is capable of communicating information to the second device exclusively and the second device is capable of decoding information from the first device exclusively (**232B**, **Figure 2**, page 5, lines 13-17, **Figures 3A** and **3B**, page 6, lines 4-6, page 3, lines 1-17).

D. CLAIM 3 - DEPENDENT

The subject matter of claim 3, which depends from claim 1, specifies that the first and second wireless bridge devices each include an internal power supply (**348**, **Figure 3A**, page 7, lines 3-4) for supplying power to the first and second wireless bridge devices respectively.

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

The ground of rejection to review on appeal is as follows:

A. GROUND OF REJECTION 1 (Claims 1-9, 12-16, and 18-20)

Claims 1-9, 12-16, and 18-20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Inoue et al., U.S. Patent No. 6,167,513 in view of Vij et al., U.S. Patent No. 6,452,910.

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-9, 12-16, and 18-20)

Claims 1-9, 12-16, and 18-20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Inoue et al., U.S. Patent No. 6,167,513 (hereinafter "Inoue") in view of Vij et al., U.S. Patent No. 6,452,910 (hereinafter "Vij").

A.1. Claims 1-9, 12-16, and 18-20

In finally rejecting the claims, the Examiner states:

> As per claims 1, 8, and 15, Inoue teaches a data processing configuration, a method, and a bridge suitable for use in a data processing network, comprising:
>
> a data processing system (Figures 3 [blocks 5a, 5b], 6 [blocks 2, 5a], 13 [blocks 23], 22 [blocks 2, 5a], 25 [blocks 2, 3 5a], 43 [blocks 2-1,5a], column 20, lines 35-44, i.e. stationary or mobile node);
>
> a network communication device of the data processing system for enabling the data processing system to communicate with a wired network, the communication device including a wired port for receiving a network cable connector (Figures 3 [blocks 1 a, 1 b], 6 [blocks 1a, lb], 13 [blocks 1], 22 [blocks 1a, 1b], 25 [blocks 1a, 1b], i.e. the stationary or mobile computers connected to the gateways as illustrated);
>
> a first bridge device having a cable connector for insertion in the wired port of the network communication device (Figures 6 [block 4a], 13 [block 4, GWa], 22 [block 4a], 25 [block 4a], 43 [block 4a]), wherein the first bridge device further includes an encryption unit for encrypting information received from the data processing system according to a predetermined encryption algorithm and a transmitter for transmitting the encrypted information (Figures 6, 13, 22, 25, 43, column 20, lines 35-44, i.e. GWa converts it into the encryption/end-to-end authentication format, encryption link format from GW0 (or GWa) to GW1 (or GWb)); and
>
> a second bridge device having a connector for insertion into a port of the wired network (Figures 6 [block 4b], 13 [block 4, GWb], 22 [block 4b], 25 [block 4b], 43 [block 4b]), wherein the second bridge device includes a receiver for receiving encrypted information transmitted from the first bridge device, and a decryption unit for decrypting received encrypted information according to a decryption algorithm that is matched to the encryption algorithm of the first bridge device (Figures 6, 13, 22, 25,

43, column 20, lines 35-44, i.e. GWb converts the received encryption authentication format to IP format) wherein the first and second bridge devices communicate (column 13, lines 27-32, i.e. master key shared between the packet encryption gateways).

Inoue does not teach where the bridges communicate wirelessly.

Vij teaches wirelessly connecting a personal area network and a local area network (column 1, lines 7-1 4).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the bridges communicate wirelessly, since Vij states at column 2, lines 34-38 that using wireless bridges allows for the seamless integration of wireless network links while still being flexible to adapt to different wireless technologies (column 1, lines 66-67).

Final Office Action dated July 19, 2007, pages 4-6.

Claim 1 on appeal herein is as follows:

1. A data processing configuration, comprising:
a data processing system;
a network communication device of the data processing system for enabling the data processing system to communicate with a wired network, the network communication device including a wired port for receiving a cable connector;
a first wireless bridge device having a cable connector for insertion in the wired port of the network communication device, wherein the first wireless bridge device further includes an encryption unit for encrypting information received from the data processing system according to a predetermined encryption algorithm and a transmitter for transmitting the encrypted information wirelessly; and
a second wireless bridge device having a cable connector for insertion into a port of the wired network, wherein the second wireless bridge device includes a receiver for receiving encrypted information transmitted wirelessly from the first wireless bridge device, and a decryption unit for decrypting the received encrypted information according to a decryption algorithm that is matched to the encryption algorithm of the first wireless bridge device, wherein the first and second wireless bridge devices communicate exclusively with each other in a wireless manner.

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). To establish a *prima facie* case of obviousness, there must be an apparent reason, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings in the fashion claimed by the application at issue. *KSR Int'l. Co. v. Teleflex, Inc.*, No. 04-1350 (U.S. Apr. 30, 2007). Additionally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka,* 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

With respect to claim 1, Appellant respectfully submits that neither Inoue nor Vij nor the combination of Inoue in view of Vij teaches or suggests first and second wireless bridge devices, "wherein the first and second wireless bridge devices communicate exclusively with each other in a wireless manner" as recited in the claim. Therefore, no *prima facie* obviousness rejection can be made against claim 1.

In finally rejecting claim 1, the Examiner states that Inoue discloses "wherein the first and second bridge devices communicate (column 13, lines 27-32, i.e. master key shared between the packet encryption gateways)." Column 13, lines 27-32 of Inoue is as follows:

> The master key to be shared between two data packet encryption gateways or between the data packet encryption gateway and the mobile computer can be generated by the exchange of a secret key or the derivation using a public key and a secret key (such as the Diffie-Hellman method), for example.

.

This portion of Inoue teaches that a master key can be generated by the exchange of a secret key or the derivation using a public key and a secret key. However, this teaching of Inoue is not relevant to whether the first and second wireless bridge devices communicate exclusively with each other in a wireless manner. For example, Inoue teaches that the master key can be communicated from the mobile computer to some other network computer. In fact, the major point of Inoue's disclosure is to provide a mechanism for a mobile computer to securely transmit information to more than one wired network. Because, in Inoue, the master key can be communicated between multiple computers in multiple wired networks, any identified "first" and "second" bridges in Inoue do not communicate with each other exclusively.

Furthermore, because the objective of Inoue is to provide a system for a mobile computer to securely transmit information to more than one wired network, causing bridges to communicate with each other exclusively would defeat the entire purpose of Inoue's system. Therefore, Inoue not only fails to teach "wherein the first and second wireless bridge devices communicate exclusively with each other in a wireless manner" as recited in claim 1, but Inoue also teaches away from the invention recited in claim 1.

Vij does not supply the above deficiencies in Inoue. Vij is cited as teaching wirelessly connecting a personal area network and a local area network, and discloses a single device for facilitating communication among disparate wireless protocols. Vij is also devoid of any disclosure regarding "wherein the first and second wireless bridge devices communicate exclusively with each other in a wireless manner."

Because neither Inoue nor Vij teaches or suggests "wherein the first and second wireless bridge devices communicate exclusively with each other in a wireless manner", the proposed combination of Inoue in view of Vij also does not teach or suggest this claimed feature. Therefore, the Examiner has not established a *prima facie* case of obviousness in rejecting claim 1, and claim 1 patentably distinguishes over the references in its present form.

Furthermore, the Examiner has failed to establish a *prima facie* case of obviousness in rejecting claim 1 over Inoue in view of Vij because no apparent reason exists to combine the references to achieve the invention of claim 1. *KSR Int'l. Co. v. Teleflex, Inc.*, No. 04-1350 (U.S. Apr. 30, 2007). In particular, no apparent reason exists to combine Inoue and Vij because the references individually and together teach away from the invention of claim 1.

As discussed above, causing bridges to communicate exclusively with each other, as claimed in claim 1, would defeat the entire purpose of Inoue's system. Inoue specifically describes:

> A mobile computing scheme capable of carrying out a proper packet transfer according to a current location of the mobile computer by accounting for the network operating policy. A mobile computer carries out a prescribed communication processing according to recognition results as to whether the mobile computer is located inside or outside the home network at which a mobile computer management device of the mobile computer is provided, and whether or not there exists a packet processing device which has a packet transmitted by at least one of the mobile computer and a correspondent computer as an encryption and authentication processing target. Also, a packet processing device carries

> out a prescribed transfer processing according to recognition results as to whether at least one of a source computer and a destination computer of a packet to be transferred is a moving mobile computer which is moving outside its home network, and whether or not there exists a packet processing device which has a packet transmitted by at least one of the source computer and the destination computer as an encryption and authentication processing target.

Inoue, Abstract.

Inoue teaches a method for processing encrypted packets when a mobile computer moves outside the mobile computer's home network. Thus, the communication bridge in the mobile computer does not communicate with a wired network exclusively. If such communication were exclusive, then one would not be able to communicate with any network except for the home network. Appellant respectfully submits that one of ordinary skill would avoid such an outcome, and, accordingly, Inoue teaches away from claim 1. For this reason, no apparent reason exists to combine or modify the references to achieve the invention of claim 1. Therefore, under the standards of *KSR Int'l. Co. v. Teleflex, Inc.*, claim 1 is not obvious in view of the combination of Inoue and Vij.

Additionally, Vij teaches away from the invention of claim 1. Vij states:

> A Wireless bridge conjoins two previously incompatible technologies within a single device to leverage the strengths of each. The Wireless bridge marries the Personal Area Network (PAN) technology of Bluetooth as described in Bluetooth Specification Version 1.0B with the Wireless Local Area Network (WLAN) technology described in the IEEE802.11a specification to provide a wireless system level solution for peripheral devices to provide Internet service interactions. The invention brings together in a single working device implementations of these technologies so they do not interfere or disrupt the operation of each other and instead provide a seamless transition of a Bluetooth connection to Wireless Local Area Network/Internet connection. From the Wireless Local Area Network perspective the inventive wireless bridge extension allows a Bluetooth-enabled device to roam from one Wireless Access Point (bridge) to the next without losing its back end connection. The invention takes into account the minimum separation and shielding required of these potentially conflicting technologies to inter-operate.

Vij, Abstract.

Thus, Vij provides for a system to allow a single wireless bridge to communicate with multiple, initially incompatible technologies. No apparent reason exists to create exclusive communication between two wireless ports because the point of Vij's system is to facilitate communication between multiple technologies. For example, Figure 5 of Vij, reproduced below, shows multiple slaved BLUETOOTH® connections between a WLAN server:

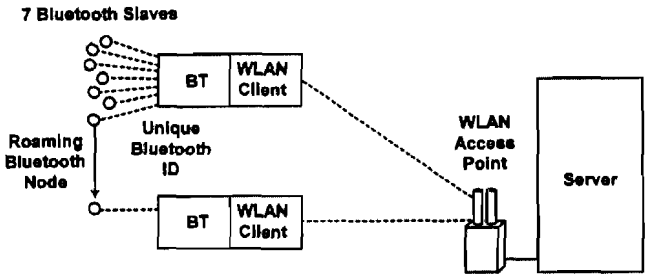

Fig. 5

Vij does state that:

> The Wireless Bridge always acts as a master. It will try to establish connection with Bluetooth-enabled vehicles or handheld devices. Prior to connection establishment, the bridge will be in Inquiry Mode and the Bluetooth Module in the vehicle or handheld will be in Inquiry Scan Mode. The Inquiry phase will be followed by Paging and Connection phases as defined in the Bluetooth Specification Version 1.0B. The Internet-connected server will try to close inactive Bluetooth connections to minimize the number of Bluetooth connections, since the maximum number of active Bluetooth connections in a piconet is seven. The Bridge will therefore respond to control command from the server. It will establish an exclusive port to the server for this purpose.

Vij, col. 8, lines 6-18.

Although Vij may teach that the wireless bridge will establish an exclusive port to the server, the server does not have exclusive communication with the wireless bridge, as required by claim 1. Again, claim 1 recites that, "the first and second wireless bridge devices communicate exclusively with each other in a wireless manner." Therefore, because Vij teaches non-exclusive communication between a server and other wireless bridges, Vij also teaches away from this feature claim 1.

Because both Inoue and Vij teach away from claim 1, the proposed combination of Inoue and Vij, considered as a whole, also teaches away from claim 1. Accordingly, no apparent reason exists to combine the references under the standards of *KSR Int'l. Co. v. Teleflex, Inc.* Therefore, the Examiner has also failed to establish a *prima facie* case of obviousness in rejecting claim 1 over Inoue in view of Vij for this reason, as well.

For at least all the above reasons, claim 1 is not obvious over Inoue in view of Vij and patentably distinguishes over the references in its present form.

Independent claims 8 and 15 recite similar subject matter as claim 1, and patentably distinguish over Inoue in view of Vij for similar reasons as discussed above with respect to claim 1. Claims 2-7, 9, 12-14, 16 and 18-20 depend from and further restrict one of the independent claims, and patentably distinguish over Inoue in view of Vij, at least by virtue of their dependency.

A.2. Claim 3

Claim 3 depends from and further restricts claim 1 and is as follows:

> 3. The configuration of claim 1, wherein the first and second wireless bridge devices each include an internal power supply for supplying power to the first and second wireless bridge devices respectively.

In rejecting claim 3, the Examiner takes Official Notice that Inoue teaches that first and second bridge devices therein "each include an internal power supply for supplying power to the first and second bridge devices respectively, since without a power supply, the bridging devices would not work." Appellant respectfully disagrees with the Examiner's conclusions. Appellant respectfully submits that neither Inoue nor Vij nor their combination discloses or suggests wherein first and second wireless bridge devices "each include an internal power supply for supplying power to the first and second wireless bridge devices respectively" and that the Examiner is making an unsupported assumption that is not disclosed or suggested by the cited art.

The Examiner, accordingly, has failed to establish a *prima facie* case of obviousness in rejecting claim 3; and claim 3 patentably distinguishes over the cited art in its own right as well as by virtue of its dependency from claim 1.

For at least all the above reasons, Appellant respectfully submits that claims 1-9, 12-16, and 18-20 patentably distinguish over the cited art, and it is respectfully requested that the Board reverse the Examiner's Final Rejection of the claims.

/Gerald H. Glanzman/
Gerald H. Glanzman
Reg. No. 25,035
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A data processing configuration, comprising:

a data processing system;

a network communication device of the data processing system for enabling the data processing system to communicate with a wired network, the network communication device including a wired port for receiving a cable connector;

a first wireless bridge device having a cable connector for insertion in the wired port of the network communication device, wherein the first wireless bridge device further includes an encryption unit for encrypting information received from the data processing system according to a predetermined encryption algorithm and a transmitter for transmitting the encrypted information wirelessly; and

a second wireless bridge device having a cable connector for insertion into a port of the wired network, wherein the second wireless bridge device includes a receiver for receiving encrypted information transmitted wirelessly from the first wireless bridge device, and a decryption unit for decrypting the received encrypted information according to a decryption algorithm that is matched to the encryption algorithm of the first wireless bridge device, wherein the first and second wireless bridge devices communicate exclusively with each other in a wireless manner.

2. The configuration of claim 1, wherein the encryption unit of the first wireless bridge device is configured to format the encrypted information according to a wireless protocol prior to

transmitting the encrypted information, and wherein the decryption unit of the second wireless bridge device is configured to unformat the wireless protocol prior to decrypting the received encrypted information.

3. The configuration of claim 1, wherein the first and second wireless bridge devices each include an internal power supply for supplying power to the first and second wireless bridge devices respectively.

4. The configuration of claim 2, wherein the first wireless bridge device further includes means for receiving and decrypting information transmitted by the second wireless bridge device, and wherein the second wireless bridge device includes means for encrypting network packets and transmitting the encrypted packets.

5. The configuration of claim 1, wherein the encryption algorithm is based on an encryption key common to and embedded in the first and second wireless bridge devices.

6. The configuration of claim 5, wherein the encryption key is at least 128 bits and unique to the first and second wireless bridge devices.

7. The configuration of claim 1, wherein the first and second wireless bridge device cable connectors are RJ-45 compliant connectors and wherein the network communication device comprises an Ethernet compliant network interface card of the data processing device.

8. A wireless bridge suitable for use in a data processing network, comprising:

a first wireless bridge device configured to receive network packets from a network communication device, encrypt the network packets according to an encryption algorithm, and transmit the encrypted packets wirelessly, wherein the first wireless bridge device includes an RJ-45 connector suitable for connecting to an Ethernet compliant NIC; and

a second wireless bridge device configured to receive encrypted network packets from the first wireless bridge device and decrypt the packets according to a decryption algorithm, wherein the second wireless bridge device is configured to connected to an RJ-45 port of a wired local area network, wherein the encryption and decryption algorithms of the first and second wireless bridge devices are unique and matched to each other wherein the first wireless bridge device is capable of communicating information exclusively to the second wireless bridge device and the second wireless bridge device is capable of decoding information exclusively from the first wireless bridge device.

9. The wireless bridge of claim 8, wherein the first wireless bridge device is configured to connect to a network interface card (NIC) of a data processing system.

12. The wireless bridge of claim 8, wherein the first wireless bridge device is configured to format the encrypted information according to a wireless protocol prior to transmitting the encrypted information, and wherein the second wireless bridge device is configured to unformat the wireless protocol prior to decrypting the encrypted information.

13. The wireless bridge of claim 12, wherein the wireless protocol is selected from an IEEE 802.11 protocol and a short range wireless protocol.

14. The wireless bridge of claim 12, wherein the first wireless bridge device further includes means for receiving and decrypting information transmitted by the second wireless bridge device, and wherein the second wireless bridge device includes means for encrypting network packets and transmitting the encrypted packets.

15. A method of enabling wireless connection between a data processing device and a local area network, comprising:

providing a first wireless bridge device configured to receive network packets from a network device, encrypt the packets according to an encryption algorithm, and transmit the encrypted packets wirelessly; and

providing a second wireless bridge device configured to receive encrypted network packets from the wireless bridge device and decrypt the packets according to a decryption algorithm wherein the encryption and decryption algorithms of the first and second wireless bridge devices are unique and matched to each other wherein the first wireless bridge device is capable of communicating information exclusively to the second device exclusively and the second devices is capable of decoding information from the first device exclusively.

16. The method of claim 15, wherein providing the first and second wireless bridge devices is further characterized as providing a first bridge device configured to format the encrypted

information according to a wireless protocol prior to transmitting it and providing a second wireless bridge device configured to unformat the wireless protocol prior to decrypting it.

18. The method of claim 16, wherein the first wireless bridge device further includes means for receiving and decrypting information transmitted by the second wireless bridge device and wherein the second wireless bridge device includes means for encrypting network packets and transmitting the encrypted packets to the first wireless bridge device.

19. The method of claim 15, wherein the encryption algorithm is based on an encryption key common to and embedded in the first and second wireless bridge devices.

20. The method of claim 19, wherein the encryption key is unique to the first and second wireless bridge devices.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.